identity theft and online scams. It is important to raise awareness of these threats and how they can be avoided.

Cybersecurity is also critical to our national security. A cyberattack against our Nation could cripple our communications, destroy our energy grids and damage our economy. We must take proactive steps today to prevent and respond to future attacks.

I also commend the Air Force for establishing a Cyber Command. Our Nation must be able to defeat any adversary on tomorrow's cyberbattlefield.

I thank my friend from Florida (Mr. FEENEY) for yielding time, and I urge my colleagues to support this resolution.

Mr. LAMPSON. Mr. Speaker, I reserve my time.

Mr. FEENEY. I want to thank my friend from California.

Mr. Speaker, I yield 4 minutes to my friend, the gentleman from Texas (Mr. MCCAUL).

Mr. MCCAUL of Texas. I thank the gentleman from Florida.

Mr. Speaker, I want to thank the Members who introduced the bill. I want to thank Chairman LANGEVIN, who I have worked with very closely on this.

Mr. Speaker, I rise today to urge the passage of this resolution, which supports the goals and ideals of National Cyber Security Awareness Month. While I believe it is important to recognize the need for cybersecurity awareness, this is an issue that should not be limited to just one month. Cybersecurity should be on the minds of all of us throughout the entire year.

Computers and the Internet have become an integral part of American business, government and lifestyle. Over 200 million Americans use the Internet on a regular basis. Companies, both large and small, rely on the Internet to manage their business, expand their customer reach and enhance their connection with their supply chain.

Almost 90 percent of all youth use the Internet, and the vast majority of those use the Internet at school. It is important that these children are taught to use the Internet in a safe and secure manner. This will not only protect their own systems from attack, but will provide for their physical safety.

Cybersecurity is also a critical part of our Nation's overall homeland security. The systems that control and monitor our dams, power grids, oil and gas supplies, as well as our transportation systems and other critical manufacturing processes, are connected to the Internet.

Right now, a terrorist organization or a hostile nation-state could disrupt our critical infrastructure systems and do serious damage to our economy without even entering our country. Appropriate cybersecurity practices are essential to overall security.

The dangers associated with online behavior are becoming more and more common. These threats range from spam, viruses and identity theft to complex computer attacks created by organized crime, terrorist organizations and possibly nation-states designed to steal sensitive information through espionage.

Organizations, such as National Cyber Security Alliance, are making it their mission to increase awareness of cybersecurity and technologies to home users, students, teachers and small businesses. These organizations deserve to be recognized for their good work and be supported.

While there is much to do, cybersecurity awareness is growing. The Congress has a role to play in encouraging the use of proper cybersecurity practices and technologies throughout our country. National Cyber Security Awareness Month provides a solid platform from which to improve cybersecurity awareness in our country, and I am pleased that this Congress is supporting its ideals and its goals. We have much more work to do, but being aware of the need for cybersecurity is a necessary first step.

Mr. LAMPSON. Mr. Speaker, I continue to reserve my time.

Mr. FEENEY. Mr. Speaker, I yield 5 minutes to the gentleman from Georgia (Mr. KINGSTON).

Mr. KINGSTON. I thank the gentleman for yielding.

Mr. Speaker, I wanted to talk a little bit about my dad. My dad is 89 years old. He has never owned a credit card. He has never even had a digital telephone. He doesn't have a computer. He doesn't have Internet. He is not interested in any of it. And yet, as removed as he might be from computer technology on a day-to-day basis, as it would appear in his personal life, the truth of the matter is, no one is isolated from high tech today.

□ 1845

His veterans payments, his Social Security payments, his bank transfers, his Medicare, all of this comes to him through computer networks. If anybody messes up those computer networks, my 89-year-old dad will not get the services that he needs. That's why this is so important today.

Today there are some 64,000 hacker programs that are available to consumers for free. In addition, there are 12,000 that if you pay $1,000 for them, you get 1 year's support. Support for a hacker program, can you imagine that. And America's computers are absolutely under siege.

I am proud that in 2002 Armstrong Atlantic University in Savannah, Georgia, began its Regional Center for Cybersecurity Education and Training. This was part of the G–8 Summit which was held in Savannah, Georgia, in 2004, and they played a key role in the law enforcement efforts surrounding the G–8.

Since then, Armstrong Atlantic University has taken on partners of Washington Group International and Bridgeborn, and they are offering all kinds of computer security training programs, from simulating and modeling to visualization, covert channels, cybersecurity and security of networks.

Why is this important? Now, Mr. MCCAUL said there are 200 million U.S. citizens connected to the Internet. It is even more than that. The numbers of people with access have increased over 182 percent from 2000 to 2005. In 2006, total nontravel-related spending on the Internet is estimated to be over $100 billion. That is a 24 percent increase over 2005. In 2005 the FBI has estimated that American businesses lost $67 billion because of computer crime, and that number of $67 billion in 2005 has moved to over $105 billion in 2007.

The United States is the location of 40 percent of the known command-and-control servers; and because of that, we are the target of attack after attack. Most of these are executed by botnets, which are a collection of broadband-enabled PCs hijacked during virus and worm attacks and seeded with software that connects back to a server to receive communications from a remote attacker. In other words, the botnets all work together to simultaneously and consistently and constantly attack computer networks, such as the Department of Defense, the Centers for Disease Control, and the Department of Energy.

In fact, in America our governmental computers alone get millions of attacks each and every day. It is something that we all should be very concerned about. The United States was the top country for malicious activity, making up over 31 percent of the worldwide total.

Personal information, for example, on veterans in May 2006 was taken home with a Veterans Administration employee, and 26 million veterans had their own personal information compromised simply because one employee took a laptop home. Now 25 years ago that may have required a truckload to carry that many files home. But just think about it, all he did was take a laptop home. And if the employee's house had not been broken into and the laptop stolen, we still might not have known about it. The Department ended up spending $200,000 a day just to operate a call center to explain to veterans how this might affect their service. Of course, there are class action lawsuits that have followed, and there will be a lot more discussion about that.

In September 2000, a 16-year-old young man in Florida intercepted 3,300 e-mails from one Department of Defense operation. He also stole 13 NASA computers.

In February 2001, Gary McKinnon of London took a poorly secured Windows system of NASA and the Pentagon and 12 other military operations and caused almost $1 million worth of damage by just basically playing around.

We know that in March 2007 Max Ray Butler, a 27-year-old computer expert